CHAPTER 6

Contested Space: The Internet And Global Civil Society

John Naughton

Introduction

The Internet offers powerful facilities for groups and organisations operating outside conventional power structures. It does this by changing the economics and logistics of information and communication. Civil society institutions were 'early adopters' of the Internet and are successfully and intensively using the network to further their goals and conduct their activities. This is not surprising given the libertarian ethos of the Net and its decentralised architecture.

However, the extent to which the Internet is being harnessed for civil society purposes is uneven. In some cases the potential of the medium has not been realised because of inequalities in access—particularly the digital divide measured in social, economic, and educational terms—government regulation or censorship, and aggressive corporate action.

We are in a transition phase in which established power structures are catching up with the libertarian and centripetal characteristics of the Net. In many cases civil society's uses of the network have been more imaginative than those of traditional institutions. But the old order is wising up. Aspects of Internet activity that only four years ago were regarded as intrinsically incapable of being regulated—for example, copyright and defamation—are rapidly being brought within the scope of national legal systems. New regulatory regimes which are intrinsically more intrusive are being implemented by legislatures across the globe, ostensibly to address the new challenges presented by the Internet but in many cases as a response to pressures from corporate lobbies and security services. And the evolution of the Internet into a mass medium has made it more vulnerable to government and corporate control.

Many of the features of the Internet which make it particularly conducive to civil society uses are a product of the network's technological architecture. But if the underlying architecture were to change, its usefulness to civil society might be reduced. There are good reasons to suppose that the rapid development of e-business poses a major threat to online freedoms because online commerce requires modification of the existing 'permissive' architecture in ways that will make it a more controlled space. It is important that civil society recognises the nature and extent of this threat, and that civil society groups formulate policies and initiatives to address it.

At the same time, other, potentially very radical Internet technologies exist or are incubating, notably public key encryption, peer-to-peer networking, the spread of persistent ('always on') broadband connectivity, and the evolution of the Web into a two-way communication medium rather than a relatively passive publication medium. By giving a new impetus to libertarian uses of the Internet, these technologies are also likely to trigger a new set of tensions between Internet 'freedoms' and regulatory pressures.

The question of whether the Internet is intrinsically a subversive technology which is immune from control by established economic and power structures is thus an open one. Recent history is not necessarily a guide to future outcomes and may even be misleading. This chapter therefore attempts to chart a contested space which is in a state of constant disequilibrium and likely to continue that way.

We begin with an outline of the architecture of the Internet and the facilities it offers to global civil society. This is followed by some illustrations of civil society uses of the Net in a number of different areas. We then consider two factors which threaten to limit the usefulness of the network in these contexts. The first is the so-called 'digital divide' and its worrying implications for those who seek to harness the Internet as a force for enlarging the space for public discussion and social action. The second is the steady encroachment of governmental and corporate agencies on the basic freedoms of the Net. Finally we examine some of the new Internet-based technologies which may tip the balance back in favour of libertarian uses of the network. The concluding section argues that global civil society has a vital stake in ensuring that the Net remains open and uncontrolled by governmental or corporate forces.

The Network

History

Although the Internet is popularly portrayed as a computer network, it is more accurately defined as 'a global network of computer networks' which operates using a set of open technological protocols of which the Transmission Control Protocol (TCP/IP) suite is the most important. The Internet works by breaking messages into small parcels of data known as packets and then passing those packets through the system until they reach their destination. TCP takes care of the disassembly of messages into packets at the transmission end and their reassembly at the receiving end. IP handles the addressing of data packets.

The current Internet[1] came into being in January 1983, having evolved from the ARPANET, a packet-switching network conceived and funded by the Advanced Research Projects Agency (ARPA) of the US Department of Defense (DoD). The ARPANET came into operation in October 1969. Although it was funded by a military budget, the prime motivation behind the network was to link research computers and researchers funded by ARPA in laboratories and universities across the US, thereby increasing the utilisation of what were at the time extremely expensive assets, namely, large mainframe computers, most of which were incompatible with one another. The prime uses of the new network were originally expected to lie in the facilitation of remote access to these time-shared mainframes and the transport of files from one location to another. One of the unexpected discoveries of the project was that the most intensive application turned out to involve the passing of messages between researchers, that is, electronic mail (Hafner and Lyon 1996: 214).

The ARPANET was a uniform system accessible only to researchers funded by ARPA. Shortly after it came into operation, a number of other computer networks came into being in the US and elsewhere. Among them were the ALOHA network in Hawaii, the Cyclades network in France, and the NPL network in the UK's National Physical Laboratory. Although all of these non-ARPA networks also used packet-switching technology, they were functionally incompatible with one another and the DoD system. After the successful demonstration of the ARPANET as a working system in 1972, therefore, ARPA turned its attention to the problem of how to 'internetwork' these networks to create a bigger, transnational network. The solution, which originated with Vinton Cerf and Robert Kahn, evolved over the decade 1973–83 and involved the creation of a set of protocols (technical conventions) which would enable computers to act as gateways between different networks so that messages could be passed reliably from any node to any other node via an indeterminate number of routing stations (Naughton 2000: 162). These protocols eventually became a 'family' of upwards of 100 detailed standards known collectively as the 'TCP/IP suite'.

The architecture of the Net

The significance of the 'internetting' technology based on TCP/IP is that it enabled the creation of a global network with an open, permissive architecture. As there was no central control, it would not make sense to try to pre-specify the kinds of networks which would be permitted to join. Anyone could hook up a network to the emerging 'internetwork' so long as they had a gateway computer which 'spoke' TCP/IP. This principle enabled the emerging network to grow organically at an astonishing speed.

An important implication of the Cerf-Kahn design was that the overall network was essentially 'dumb'. Its only function was to pass electronic packets from one point to another: the so-called 'end-to-end' principle.[2] As far as the network was concerned, those packets might be fragments of e-mail, photographs, recorded music, or pornographic videos: they were all the same to the network and were treated identically. This indifference to content made the Internet—the term 'internetwork' was quickly shortened to the less cumbersome 'Internet'—radically different from previous communications networks which had been owned or controlled by agencies that determined the uses to which their systems could be put. In the UK and many European countries,

[1] *The term 'Internet' is often used synonymously with other terms like 'Web'. For our purposes, the Internet is treated as the communications infrastructure along which various kinds of communications traffic—electronic mail, Web pages, digitised files (MP3, voice, video, text, and so on)—pass.*

[2] *The 'end-to-end argument' was articulated by network architects Jerome Saltzer, David Reed, and David Clark in 1981 as a principle for allocating intelligence within a large-scale computer network. It has since become a central principle of the Internet's design. See Stanford Center for Internet and Society (2000).*

for example, the national telephone networks were owned for most of the twentieth century by national post offices, which partly explains why FAX technology was so slow to take off in the West: organisations devoted to delivering letters by hand were not disposed to promote the idea of sending letters down a telephone wire. In sharp contrast, uses and applications of the Internet were determined entirely by the ingenuity of its users and those who developed applications which could harness its message-passing capabilities. Some commentators (for example, Lessig 1999*a*) have attributed the explosion of economic activity and creativity generated by the Internet to this factor.

The other feature of the original Internet architecture which is significant for our purposes is the fact that authentication of users was not required. Each machine connected to the Net needed to have a unique 'IP' (Internet Protocol) address,[3] and all of that machine's transactions with other machines on the network could be logged. But there was—and currently still is—no provision for linking IP addresses to known individuals. This meant that the architecture facilitated anonymity: a feature famously encapsulated by the celebrated 1993 New Yorker cartoon showing two dogs in front of a computer. 'On the Internet', one is saying, 'nobody knows you're a dog'.

The implications of the architecture's facilitation of anonymity have been far-reaching. Anonymity is a two-edged sword. On the one hand it permits a wide range of reputable (and disreputable) uses of the Net because the identity-based sanctions of the real world do not apply in cyberspace. On the other hand, anonymity often enables the free expression and dissemination of views in ways that would be more difficult in real-world arenas. The architecture makes it difficult, for example, for security services to track down or silence dissidents and for corporations to identify whistle-blowers or campaigning groups disseminating critical information or hostile propaganda.

The technical architecture of the Net has thus been a prime determinant of how the network has been used. As in the physical world, architecture enables some things and prevents others. The significant point from our point of view is that the architecture of the Net is cast in terms of technical protocols, that is to say, as computer code. And, as Lessig (1999*b*) has pointed out, there is nothing immutable about code. It is pure 'thought-stuff' and as such can be changed. This is a subject to which we will return.

Table 6.1: Estimated internet user population, November 2000

Region	Users (millions)	% of total
Africa	3.11	0.76
Asia/Pacific	104.88	25.76
Europe	113.14	27.79
Middle East	2.40	0.59
Canada and USA	167.12	41.05
Latin America	16.45	4.04
World Total	407.10	

Source: Nua Internet Surveys (URL) For country data see table R10 in part IV of this yearbook.

Scale

The Internet is a global system in that it has nodes in virtually every country, but the density of users and connections is very uneven across the globe. It is estimated, for example, that 69 per cent of Internet users are located in North America and Europe, and that Africa, with 13 per cent of the world's population, has less than 1 per cent of the world's Internet users.

Nevertheless the scale of the network's coverage is still remarkable. Because of the 'organic' architecture created by the TCP/IP protocols, it's impossible to say how many Internet users there are, but authoritative estimates at the time of writing (February 2001) suggest numbers in the region of 400 million.

The Internet as a communications space for global civil society

Although there are arguments about its long-term significance, few doubt that the Internet represents a radical transformation of mankind's communications environment. As one well-known Net evangelist (Barlow in Barlow *et al.* 1995) has said, 'We are in the middle of the most transforming technological event since the capture of fire'. There is a widespread belief

[3] *A number made up of four sets of digits: for example, 255.212.12.40. Computers accessing the Net via dial-up lines are assigned temporary IP addresses from a bank held by their Internet services provider (ISP). Computers on local area networks generally access the Net through a gateway machine so that all transactions by an individual machine are logged against the IP address of the gateway computer.*

that in areas where 'information is power' the rise of the Net has to some extent levelled the playing field on which marginalised and grass-roots organisations compete with established economic, media, and governmental interests for public attention.

Most of the evidence for this is anecdotal, if only because there has as yet been little systematic empirical research on the subject. But an examination of the communications capabilities of the Internet suggests some good reasons for supposing that the conjecture is plausible.

As a communications space, the Internet:

- facilitates access to published data, information and knowledge;
- lowers the barriers to publication and enables groups and individuals to bypass traditional gatekeepers in media and publishing;
- facilitates rapid communication on a global scale;
- facilitates the sharing of information resources; and
- facilitates the formation and maintenance of 'virtual communities' of people or institutions with shared interests.

Access to published data, information and knowledge

The volume of data and information now published on the World Wide Web (WWW) is phenomenal, and indeed threatens to overwhelm the capacity of search engines and directories to index and categorise it. In February 2001, Google (URL), a leading search engine, was claiming to index 1.3 billion Web pages, which it estimated to be about half of the total number of Web pages published at that time. Other estimates of the total number of Web pages are higher. More significant than the sheer volume, however, is that fact that an increasing proportion of government, official, institutional, and corporate publications are now routinely published on the Web. Although many of these publications have previously been available in print, the practical effect of online publication has been greatly to increase the accessibility of such documents. For example, Hansard, the daily transcript of proceedings in the UK Parliament, has always been available in print to those who had the resources to purchase or physically access the printed edition, which in practice meant those with ready access to a major library in the United Kingdom or one of the very few national libraries which have such holdings. Now Hansard is published daily on the Web, with the result that anyone anywhere in the world with a browser and an Internet connection can access the British parliamentary record. Similarly with major public documents such as the report of the inquiry into the BSE (URL) epidemic in Britain.

Much the same applies in other countries— for example, the US—where transcripts of congressional sessions, court proceedings, legal judgments and pleadings, and so on are available online. Instead of relying on local media reports, an environmental activist in Asia or Europe can now immediately access the exact text of President Bush's rejection of the Kyoto Protocol, for instance. Most significant UN publications are now published on the Web. Given that many civil society activities are about widening the scope of public debate about controversial issues and that interpretations of official data and information are a critical input to this process, online publication has been a boon for this sector. It has also much facilitated local and national activism on global issues, as activists can compare the policies of different governments and international organisations when deciding how to approach their own authorities.

Lowering barriers to publication

For many civil society applications, online publication is preferable to publication in traditional media because it is relatively inexpensive, provides global coverage, and bypasses the gatekeepers who control access to traditional media. It makes it possible, for example, to publish an attractive, full-colour pamphlet and distribute it globally at a cost which is determined almost entirely by the remuneration required by those who produce it. There is no need to set up a distribution network; and distribution costs are paid by readers. Furthermore, online publication is not limited simply to documents. Anyone with a modicum of skill and a simple recording device—for example, minidisc recorder, still camera, video camera, scanner—can create audio, photographic, or digital files which can be loaded onto a Web server and made available for download to all comers, again on a global basis—though of course there are channel capacity (bandwidth) limitations: users with slow dial-up connections will take much longer to access non-text files. The Internet thus lowers the barriers not just to document publication but also to multi-media publication.

The Internet makes it increasingly difficult for governments to maintain secrecy or prevent—for example, by legal injunction—publication within their jurisdictions. In the 1980s, for example, the British government successfully used legal methods to prevent Spycatcher—the memoirs of Peter Wright, a former MI5 officer who alleged that the security service had conspired to undermine the British Labour government led by Harold Wilson in the 1960s—from being read by British subjects, even though the book had been widely published abroad. Newspapers which attempted to publish excerpts were made subject to legal injunctions and British residents who wished to read Wright's allegations had to resort to absurd measures like making a day-trip to the Irish Republic in order to obtain a copy. This would be unimaginable today.[4] At the first sign of a British or European injunction the contents of the book would appear on a Web-server in the US where they would enjoy the protection of the First Amendment and be available to anyone with a browser and an Internet connection.

Rapid and inexpensive communication on a global scale

The Internet offers a wide range of facilities for individual and group communication and discussion.

Electronic mail and discussion lists. E-mail and discussion lists are the oldest, most popular, and lowest-tech forms of interaction on the Internet. E-mail is a classic person-to-person medium and represents the way in which most Internet users actively engage with the network. For example, one authoritative survey (The Pew Internet and American Life Project URL) estimates that 49 per cent of US Internet users send one or more e-mail messages a day.

For group purposes, the most significant development of e-mail technology is the 'list server', that is, a program, sometimes called a ListServ, which enables people to subscribe to a discussion list and receive by e-mail messages that the list owner or other subscribers have posted. When people send messages and responses to a list, an online discussion can develop. The number of discussion lists currently active is unknowable but is certainly very large[5] and they are a prime resource for civil society groups.

E-mail lists have certain characteristics which distinguish them from other kinds of Internet-based discussion systems. They are, for example:

> *typically owned by a single individual or small group. Since all messages to a list must pass through a single point, email lists offer their owners significant control over who can contribute to their group. List owners can personally review all requests to be added to a list, forbid anyone from contributing to the list if they are not on the list themselves, and even censor specific messages that they do not want broadcast to the list as a whole.*
> *(Kollock and Smith 1999: 5)*

Since most lists thus operate as 'benign dictatorships', they are often characterised by their more orderly and focused activity than other online discussion forums.

An important feature of e-mail is that it is an asynchronous medium—sender and recipient do not have to be connected at the same time in order to communicate. This means that it is particularly useful for communicating across time zones. It is also, in general, extremely quick. Most messages reach their destination inboxes in minutes or less. E-mail is, therefore, an exceedingly powerful medium for alerting large numbers of people to new developments, which is why it has enabled global civil society groups to respond rapidly to events and often to outpace and outflank established power structures. For example, Amnesty International has launched an online network, Fast Action Stops Torture (FAST URL), as part of its worldwide campaign to stop torture. When the organisation learns of an imminent threat of torture, FAST instantly sends out an alarm to its network of activists around the globe, requesting activists by the thousands to sign electronic letters of protest. In this way a threat of torture can be exposed within hours. The rationale is that exposing torture makes it more difficult to carry out.

Asynchronous conferencing systems. The Internet also provides other forms of asynchronous discussion/conferencing systems. The most prominent is Usenet, a global system of online conferences called 'news groups' because originally they were used for circulating news about bugs and updates to managers of Unix systems; but there are proprietary equivalents run by Internet service providers (ISPs) like AOL and MSN. These allow participants to create topical groups

[4] *Compare, for example, the use of the Internet in 2000 by a disaffected MI5 operative, David Shayler (URL) to publicise his case.*

[5] *See http://www.liszt.com/ for a directory.*

in which a series of messages akin to e-mail messages can be strung together to form discussion 'threads'. Usenet-type systems are 'pull' media in the sense that people have to subscribe to conferences and then pull down from a News server the messages that interest them. In order to access newsgroups a user needs (1) a special 'client' program called a Newsreader, freely downloadable from the Net or provided in many e-mail programs, and (2) access to a News server (usually provided by one's ISP).

Usenet is, like the Internet itself, a self- organising system which operates on the basis of agreed protocols, in this case a standard message format. Something like 45,000 discussion groups, devoted to every conceivable specialism and interest, currently exist, each containing anything from a dozen to thousands of messages. On an average day tens of thousands of Usenet subscribers submit messages to the system. A new site 'joins' the Usenet by finding an existing site that is willing to pass along the daily 'feed', that is, the collections of messages *it* receives. No one 'owns' Usenet; there is no central authority, no institution that can police behaviour or enforce standards of behaviour. Virtually anyone can subscribe to a newsgroup, read all the messages on the conference, or contribute new messages. This makes the Usenet:

> *a more interesting and challenging social space than systems that are ruled by central authorities. Whatever order exists on the Usenet is the product of a delicate balance between individual freedom and collective good. Many newsgroups are wild, unordered places, but what is startling is how many are well organized and productive.*
> *(Kollock and Smith, 1999: 6)*

The main limitation in practice is whether your ISP agrees to carry the particular newsgroups in which you are interested. In practice this is one of the important 'choke points' which gives leverage to corporations and governments seeking to curtail online discussion.

Chat systems. So-called 'chat' systems enable various kinds of synchronous conversation. By far the most widespread technology is that of 'text chat' in which a number of people exchange typed messages in real time in a shared virtual space known as a 'chat room'. Although proprietary networks like AOL and MSN derive a considerable part of their revenues from the chat facilities they provide, the majority of chat interactions take place via the non-proprietary Internet Relay Chat (IRC). IRC (URL) has been described as 'the net's equivalent of CB radio'. Like CB, chat systems tend to have a great number of channels, that is, chat rooms. But unlike CB, which is localised in coverage, chat enables people all over the world to participate in real-time conversations.

Using an IRC 'client' program—freely downloadable from the Net—or proprietary clients provided by ISPs like AOL or MSN, participants exchange text messages interactively with other people via a chat server. Conversation consists of typed messages that are instantly sent to other participants. The fact that chat systems require a central server grants the server owner a great deal of power over access to both the system and individual channels. AOL's chat facilities, for example, are policed by staff or appointed volunteers (Lessig 1999*b*: 68). And even in the non-proprietary IRC each channel has an 'owner' who can control access (Kollock and Smith 1999:6).

In recent years, as modem speeds and the bandwidth of Internet connections have increased, systems which permit voice chat and even primitive video-conferencing have become popular. Excite Voice Chat, for example, enables users with multimedia-capable personal computers (PCs) —that is, computers equipped with sound cards, speakers/headphones and a microphone—to hold audio conferences with up to nine other people. And systems such as Microsoft's NetMeeting enable one-to-one video-conferencing over the Net. Performance of these non-text systems is, however, critically dependent on the quality and bandwidth of participants' Internet connections.

Web-based conferencing and chat. Although the software required for accessing Usenet and Chat is relatively easy to use, downloading and installing client software represents a challenge for many Internet users. Because most users find using a Web browser relatively unproblematic, however, there is an increasing trend to providing interactive services via the Web. Thus many of the Usenet groups can be accessed via a Web interface[6] which also provides search facilities allowing one to look for topics over the entire Usenet system: facilities that are not available via the classic Newsreader client.

Instant messaging. This is a relatively new communications service that enables an Internet user

[6] *Available at http://www.groups.google.com*

to create what is in effect a private chat room with another individual. Typically, the Instant Messaging (IM) system alerts the user whenever somebody on her private list is online. She can then initiate a chat session with that particular individual. IM has proved remarkably popular since its introduction some years ago because it is a useful technology for keeping friends and colleagues in touch with one another. At present there are several competing IM systems and no over-arching standard, so people who want to send messages to one another must use the same instant messaging system. And of course IM technology still depends on there being a central server which brokers connections between IM subscribers.

Sharing of information resources

Because of the ease of publication discussed earlier, the Internet makes it much easier for groups and individuals to share information resources. Archives of documents and other resources can be digitised and placed on Web or File Transfer Protocol (FTP)[7] servers from which they can be accessed by anyone with the appropriate permissions.

The hyper-linking technology of the Web makes it easy for collaborating organisations to compile indexes and guides to one another's materials without having to maintain multiple archives. This facility is widely used by civil society groups.

And although the growing volume of Web pages continues to outpace the capacity of search engines to index and categorise them, there are some powerful general search engines like Google (URL) which enable users to locate a high proportion of relevant documents for many types of search. Because of growing concerns among civil society institutions about bias in indexing algorithms—that is, the procedures and criteria search engines use to rank pages (Introna and Nissenbaum 2000)—some organisations—for example, OneWorld—are now creating specialist search engines which attempt regularly to survey and comprehensively index sites in their areas of concern.

Given that information is such a vital ingredient in civil society activities, one would expect that the facilities provided by the Internet for sharing and aggregating information would be universally welcomed. But according to Jonathan Peizer this is not necessarily the case, at least in the NGO sector.

> *NGOs have historically survived by owning their information and that of their constituents. This constituted their value and substituted for significant financial assets. Yet this behaviour is antithetical to effectively leveraging the Internet to meet their missions. Because of resource constraints, many continue to be behind the technology curve. The technology is not intuitive, and many NGOs don't have the requisite experience with it. Consequently, many still mistakenly judge their organization's value on pre-Internet criteria and modes of operation.* (Peizer 2000)

On this analysis, the challenge for NGOs is realising that information once unique to them may now be widely available over the Internet. The new information sources may be qualitatively better, worse, or similar, but if their providers are using their Internet presence effectively and developing online communities around it, they directly challenge the continued viability of groups which are not doing so.

Virtual communities

The literature on 'virtual communities'—social groups which conduct most of their relationships in cyberspace—is confused and confusing (for a survey see Wellman and Milena 1999). Much of the discussion focuses on the question of whether such communities are the same as 'real' communities, that is, social groupings, usually based on geographical location, to which people belong in the real world.

This is in part a continuation of old arguments about the impact of technology—as well as of bureaucratisation, urbanisation, and capitalism—on community. The current debate about the relationship between the Net and social life fits neatly into this tradition. The likelihood is, however, that once the 'fascination of the new' has palled we will discover that there is less of a dichotomy between online and real-world communities than is currently supposed. Even what we think of as normal, place-oriented communities 'can stretch well beyond the neighborhood' (Wellman and Milena 1999: 169). And one of the few ethnographic studies (Miller and Slater 2000) suggests that 'we need to treat Internet media as

[7] *One of the oldest Internet protocols, FTP provides a relatively fast and reliable way of exchanging files over the Net. Most software downloads are handled by FTP.*

continuous with and embedded in other social spaces', implying that people use the Net in ways that complement rather than disrupt their social lives. This view is supported by William Mitchell (1995), who objects to the suggestion that we must 'choose between participating in place-based communities and joining electronically supported, virtual ones—that it's one or the other. But that's just not the case. It's more accurate to say that bodily presence and telepresence now play differing, and potentially complementary roles in sustaining the connections that matter to us'.

A more productive approach might be to follow Howard Rheingold (1995), one of the earliest and most persuasive writers on the subject, and define virtual communities as 'communities of interest facilitated by computer networks'. On this definition, there are thousands, perhaps tens of thousands, of virtual communities centred on civil society activities, interests, and beliefs. The key question is whether such groupings constitute 'a way of revitalizing civil institutions through civil communications, or are they fostering a dangerous illusion of civil association that doesn't have an effect in the world where things like liberty matter' (Rheingold 1995). The experience of civil society is that virtual communities, mediated and linked by the Internet, can have real effects in terms of influencing real-world events.

Civil Society Uses of the Internet: Some Snapshots

> *The Internet has become a vitally important area for civil society. While more powerful political and economic interests dominate traditional media, the Internet has allowed the voices of ordinary citizens and organisations lacking strong financial resources to be heard. We live today in an era of globalisation, distinguished by the emergence of giant multinational corporations and unelected bureaucracies with the power to make decisions that have profound effects on people all over the world. The Internet, with over 200 million users worldwide, provides a unique public sphere where decisions that shape all our lives can be freely debated and considered. Global communities can be built there that are able to limit the power of corporations, bureaucracies and governments. In a globalised world that continuously undermines localised democratic institutions the Internet provides an essential means for defending and extending participatory democracy.*
> *(GreenNet URL)*

Given the scope of global civil society, it would be unrealistic to attempt a comprehensive survey of its uses of the Internet. Instead this section provides an impressionistic snapshot by focusing on the ways in which civil society groups working in different areas have used the medium to achieve their diverse goals.

Oneworld.org: a civil society portal

OneWorld is the largest civil society 'portal' on the Internet. It was set up in 1995 by Anuradha Vittachi, a Sri Lankan journalist specialising in human rights and development issues, and Peter Armstrong, a British-born journalist who had previously worked for BBC television. Both had worked for five years previously in more conventional publishing media, including CD-ROM, and were concerned to 'harness the democratic potential of the Internet to promote human rights and sustainable development'. OneWorld's stated aim is to be 'the online media gateway that most effectively informs a global audience about human rights and sustainable development'. But it also seeks to provide a focus for cooperation between like-minded civil society groups: 'to bring together a global community working for sustainable development through interactive online partnerships of organisations and individuals sharing our vision' (OneWorld URL).

OneWorld began with 22 partner organisations and now has over 900, many of which supply material for publication in over 80 subject categories on the OneWorld site. In order to be admitted to partner status, an organisation must be working in the fields of sustainable development or human rights, or be branches, departments, or projects which work in the fields of sustainable development or human rights as part of larger organisations with wider aims. However, where the wider organisation is seen to significantly contravene the aims of the OneWorld community, for instance by using violence or advocating intolerance on the grounds of ethnicity, gender, sexual orientation, or religion, the application will be refused. At the time of writing, OneWorld

was giving special priority to partnership applications from NGOs based in the South.

The OneWorld site now attracts over a million page views[8] a month and reaches Internet users in over 90 countries. The site publishes in five languages (English, German, Dutch, Italian, and French); it also serves as a hub for campaigns on such issues as climate change, the role of the IMF and the World Bank, and the digital divide; and runs seven specialist 'channels' on Third World Debt, learning, media, radio, TV, photography, and children. One of the aims of the radio and TV channels is to act as a not-for-profit news and features agency by providing informed broadcast material on sustainable development or human rights which can then be reused by partner organisations in ways that further their own local objectives.

Human rights on the Net

Since the appearance of the World Wide Web in 1993 there has been a veritable explosion of human rights (HR) information on the network. A crude search on Google using the keywords 'human rights' conducted on 16 April 2001 turned up 2,380,000 pages. A search on 'human rights campaigns' produced 346,000 pages. A very large number of NGOs are now online and publishing their materials, and international organisations have also begun to make large portions of their materials available online, making research much easier than in the past and enabling ready access to texts of legislation, treaties, resolutions, reports by special rapporteurs, and other essential documentation. Many academic and legal journals also offer at least some of their articles in online formats. The expansion of the Web, however, has also meant that finding materials is more difficult for those not already familiar with the major HR sites.[9]

One study (Case 1999) of the use of the Net by HR campaigners identified a number of distinct types of use:

- e-mail and discussion lists as a way of transmitting information reliably to individuals or large audiences;
- Web sites as publication platforms and sources of reliable information;
- combined use of e-mail and Web sites in conducting HR campaigns; and
- nurturing human rights communities both online and in the real world.

Case also discusses the limitations of the Net in HR work and the need for an international covenant to protect those who use it for such purposes.

It is clear that the Internet has been a boon for HR campaigners. Its facilities enable them to access official information easily and to publish information without going through the gatekeepers who control access to more traditional publishing media. E-mail and discussion lists enable them to communicate relatively easily with other activists, to make protests to government ministers and officials, to share information with large communities of like-minded people, and to alert other activists quickly—as, for example, in Amnesty International's FAST (URL) system discussed earlier—in the light of new or unexpected developments. Combinations of e-mail and Web publication make it easier to mount effective campaigns without the huge costs of traditional campaigning. And conferencing and chat technologies help to support virtual communities of activists.

The role of the Internet in coordinating protest

The use of the Internet by civil society campaigners such as the protesters who disrupted the 1999 meeting of the World Trade Organisation (WTO) in Seattle has become the stuff of media legend. Journalists marvelled at the sight of activists sending e-mail dispatches and streaming live video and audio reports from tear-gassed streets. But this was essentially a reflection of the *naïveté* and technological ignorance of mainstream media. Given that the Internet offers campaigners a communication system which is cheap, reliable, ubiquitous, efficient, and uncontrolled, it would be astonishing if they did *not* make extensive use of it, especially when it is clear that many governmental and corporate organisations do not!

The real significance of the events surrounding the Seattle WTO meeting lay not so much in

[8] *A 'page view' is the accessing of a Web page. A page view differs from a 'hit' by counting only the number of times a page has been accessed, whereas a hit counts the number of times that all the elements in a page, including graphics, have been accessed. Some Web pages can have a dozen or more graphical elements. Page views, however, have become harder to gauge, since pages can include frames that divide them into separate parts*

[9] *For an excellent guide to sources see Derechos Human Rights (URL).*

protestors' reliance on communications technology as in what the technology enabled them to do. To appreciate this one has to remember that one of the biggest challenges faced by civil society in recent decades is the way global capitalism, as manifested in bodies like the WTO, has succeeded in presenting an increasingly unified front to the world. This had rendered it apparently impervious to the countervailing activities of hundreds of thousands of isolated and uncoordinated opposition groups ranging from environmental campaigners to human rights and fair trade activists to trade unions and consumer groups. It was not as if (*pace* Fukuyama) opposition to the forces of economic globalisation did not exist: merely that their combined pressure was always less than the sum of the parts.

The Seattle meeting was significant because it showed how the Internet may be changing that. It demonstrated the synergistic possibilities when many of the disparate civil society groups opposed to organisations like the WTO use communications technology to coordinate their efforts. In the words of one observer, 'The Internet and e-mail enabled the predominantly small, non-profit groups with tiny budgets to orchestrate a massive protest among thousands of people in the United States and abroad. It also provided a link among about 150 chapters of various groups scattered on college campuses across the country' (Arnett 1999). What the WTO officials gathered in Seattle realised was that the opposition suddenly seemed greater than the sum of its parts.

Furthermore, the most important coordinating function of the Internet in this context is not so much tactical, as the traditional mass media assume, but strategic, that is, in enabling participating groups to exchange information, prepare position papers, lobby local legislatures, and generally lay the groundwork for more established forms of political action. In that sense a more instructive case study might be the role played by civil society groups in influencing the outcome of the negotiations over the proposed Multilateral Agreement on Investment (MAI).

The MAI is discussed more fully elsewhere in this volume (see Desai and Said, chapter 3 p. 60–61), but it does have an interesting Internet dimension. To recapitulate briefly: in 1997 the countries of the Organisation for Economic Cooperation and Development (OECD) began negotiating an agreement behind closed doors to set up a global framework of rules on investment. The aim was to prevent governments from favouring domestic investors and to remove restrictions on multinational corporations investing in developing countries. The intention was to give cross-border investors greater protections than those provided by the North American Free Trade Agreement (NAFTA) and the Uruguay Round agreements that established the WTO. The effect of the proposed Agreement would have been to erode national sovereignty over economic and fiscal policy in certain respects.

Publication of the MAI proposal on the Net prompted the formation of a loose coalition of NGOs including environmental organisations, consumer groups, trade unions and religious groups to question and attack the proposed agreement and expose its shortcomings and hidden agendas. By the end of 1998 there were vociferous campaigns against the agreement in half the OECD countries participating in the discussions and many more in developing countries most likely to be affected by it. Under the pressure of this publicity the negotiations collapsed.

Many participants and observers regard the networking of civil society opposition as decisive in bringing about this outcome. 'The story of the MAI', writes one:

> *is a cautionary tale about the impact of an electronically networked global civil society. The days of negotiating international treaties behind closed doors are numbered, if not over. A much broader range of groups will have to be included in the globalization debate, and much more thought will have to be given to how non-participants will interpret international negotiations and agreements.* (Kobrin 1998)

Environmental campaigning on the Net

Environmental groups were early and intensive users of the Net. One well-known directory (Kestemont 1998) lists over 620 major Web sites providing information, links, and contacts on environmental issues. A Google search on the keywords 'environmental pollution' turns up over 900,000 sites or pages. A similar search on 'global warming' returns over 400,000 hits. One on 'toxic waste' returns over half a million documents. Because much environmental campaigning requires access to scientific information, the increasing tendency of scientific researchers to publish on the Web as well as in

specialist journals makes it easier for environmental groups to locate the kind of information needed to underpin campaigns or to buttress and inform arguments to be used in offline discussions with legislators and companies. There are striking similarities between the way environmental and human rights activists use the Internet to disseminate information, publicise and conduct campaigns, issue e-mail 'alerts', and put together rapid-response campaigns.

Uneven Playing Fields: Access and the Digital Divide

The Internet, as we have seen, has brought unprecedented benefits for civil society. The facilities it provides for accessing information, communicating, publishing, and organising evince a tremendous democratising potential. The network appears to promise the realisation of Thomas Paine's dream of a society in which everyone has a voice: a true Jeffersonian market in ideas. If this dream is ever to be fully implemented, however, a fundamental problem will have to be addressed and solved. This is the issue of inequality of access to the Internet: the so-called 'digital divide', the term popularly used to describe the gap between the 'information rich' and the 'information poor'. If the benefits and facilities of the Net are available only to a selected few, then its democratising potential, not to mention its economic potential, will never be realised.

At the moment, these benefits are available only to a select minority of mankind, variously estimated at between 2 per cent and 6 per cent of the global population.[10] The digital divide operates both within societies and between regions and countries. 'Current access to the Internet runs along the fault lines of national societies, dividing educated from illiterate, men from women, rich from poor, young from old, urban from rural' (UNDP 1999: 62).

But the digital divide also has an international dimension. According to the UNDP (1999), in mid-1998 the industrial countries of the world accounted for 88 per cent of all Internet users, despite having only 15 per cent of the world's population. At the time the UNDP report was published, North America, with 5 per cent of the people, had more than 50 per cent of Internet users. And South Asia, home to 20 per cent of the world's population, had less than 1 per cent of the planet's Internet users.

Table 6.2: Teledensity in selected countries

Country	Teledensity (telephone mainlines per 100 people)
Monaco	99
United States	64
Italy	44
United Arab Emirates	40
Costa Rica	17
Kenya	0.8
Sierra Leone	0.4
Bangladesh	0.3
Uganda	0.2

Source: International Telecommunications Union (1998)
For more comprehensive data see table R10 in part IV of this Yearbook

These disparities are well known, as are the reasons for them. Internet access requires technological, social, and educational infrastructures which are unevenly distributed across global society. On the technological side, for example, the key element to date has been access to a telephone network. Using 'teledensity' (the number of telephones per 100 people) as a measure we find huge disparities in access, as Table 6.2 demonstrates.

The existence of a suitable communications infrastructure is a necessary but not sufficient condition for ensuring equality of access to the Internet. A broadband network connection is useless to someone who is illiterate. The ability to tap into and harness the information and communication resources of the Net is predicated on literacy and education. This implies that tackling the digital divide is not just a matter of creating telecommunications infrastructures where none previously existed, but also of developing universal literacy programmes and building up social capital generally. Of the two tasks, the former is likely to be the simpler to accomplish, especially given the development of wireless technologies which are much less resource intensive than conventional landline telephone networks. The inescapable conclusion is that the gap between the

[10] *The 1999 Report of the UN Development Program (UNDP) estimates that only 2 per cent of the world's population had Internet access in mid-1998. Higher estimates are based on a user population of 400 million.*

information rich and the information poor is unlikely to narrow in the medium-term future and may even widen as Internet penetration in industrialised societies gathers pace.

This is very bad news from any perspective. In economic terms, it means that under-developed societies will continue to be denied the economic benefits of the Net. Just to give one illustration, UNDP (1999:58) points out that the cost of sending a 40-page document from Madagascar to Côte d'Ivoire is $75 by five-day courier or $45 by 30-minute fax, whereas the same document can be sent by e-mail for about 20 cents—not to mention the fact that it can be dispatched to multiple recipients all over the world for the same cost.

The digital divide is also bad news in terms of human rights. Western countries have increasingly regarded universal access to telecommunications services as an important public goal (it was first written into US federal telecommunications law in 1934). The European Union requires countries seeking membership to implement policies and legislation aimed at enabling universal access to telecommunications services. The 1948 Universal Declaration of Human Rights declared that everyone has the right to freedom of expression and the right to 'receive and impart information and ideas *through any media* and *regardless of frontiers*' (emphasis added.) The digital divide implies that, in a world increasingly dependent on networked information, this right will be anything but universal for a large proportion of the global population.

The implications of the divide for global civil society are profoundly depressing. What it means is that the Internet is—and is likely to be for the foreseeable future—heavily dominated by the information-rich North/West and by very small elites in the South. This sombre reality clashes with the egalitarian aspirations ('All men are born free and equal in dignity and rights', to quote the Universal Declaration of Human Rights again) of global civil society. While Internet and computing technologies may have levelled the playing field for global civil society vis-à-vis governments and corporations in the industrialised world, it may actually have further tilted the playing field from South to North.

The Emperor's New Clues: The Battle to Control The Net

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*
>
> *We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear . . .* (Barlow 1996)

In the beginning: anarchic creativity

The Internet, as we have seen, emerged from the ARPANET, which itself was a product of the 1960s. Although its early development was funded by the military, the network was designed and built—and for the most part used—by academic researchers who inhabited a liberal, uncommercialised organisational culture. In the decade 1983 to 1993—in other words, from the launch of the TCP/IP-based network to the release of the first graphically-oriented Web browser—the Internet was essentially an intellectual sandpit and working environment for academic researchers. Its operating costs were borne by government funding agencies like the Defense Advanced Projects Research Agency (DARPA), the US National Science Foundation (NSF), universities, or the research funding councils of other countries. Most computers on the network were based in research laboratories and offices and had fast permanent connections rather than slow dial-up links. And although there were official rules and regulations about what the network could and should be used for, in practice there was little supervision and applications were limited only by the ingenuity of users. So long as the application involved the passage of data packets, the Internet would—and did—handle it.

The result was not just an explosion in creativity (Lessig 1999*a*) but also the evolution of a free-wheeling, anarchic, non-commercial, permissive ethos

sometimes summarised by the phrase 'geek culture'. It was this ethos that found expression in John Perry Barlow's celebrated 'Declaration of Independence' quoted at the start of this section. Geek culture, however, went largely unnoticed in the outside world. Because there was no commercial activity on the Net, the business world paid little attention to it. And because the community of Internet users was relatively small and cloistered, governments were even less interested.

Because many civil society groups had roots in, or connections to, academia they were early and enthusiastic users of the Net. Far from being repelled by the techno-anarchism and libertarianism of the geek culture, many activists actively welcomed it, perceiving in it resonances with their own values. The result was that civil society users of the Net were often ahead of the adoption curve as progressive and imaginative groups recognised how suitable it was for their purposes.

The release of the Mosaic browser in the Spring of 1993 led to a sea change in commercial and governmental attitudes to the Net. Mosaic was significant because it made it easier to place pictures on Web pages. Where there were pictures, there was the possibility of entertainment. And where there was entertainment there was the prospect of commercial profit, especially when it was perceived that the Web was the 'fastest-growing communications medium in history' (Naughton 2000: 27), reaching its first 50 million users in four years—as compared with 36 years for radio and 13 for television. It began to dawn in the minds of legislators and businesspeople that this phenomenon was too important to be left to geeks.

The initial intrusions of business and government into the Internet were clumsy and ill-conceived and appeared to confirm the contemptuous disdain of the Internet community towards anyone with a profiteering or regulatory mindset. A kind of complacent arrogance took hold, based on the assumption that cyberspace was somehow different in kind from 'real' space, that it was intrinsically subversive of established ways of doing things, and that it lay beyond the reach of conventional control structures. Within the cyberlibertarian community, for example, it was widely believed that censorship would always be impossible on the Net. John Gilmore's (1996) observation that 'the Internet interprets censorship as damage and routes around it' captured this sentiment precisely. This conjecture may have been reasonable at the time, but events have not borne it out: the Internet is potentially more susceptible to political and commercial control than was once thought. Cyberspace will not remain a 'digital commons' without vigorous political action to defend its freedoms. Left to their own devices, the forces of official regulation and commercial exploitation will gradually enclose the common. And this will have significant implications for global civil society.

The ambivalence of power: governments and the Net

All governments, including those in Western democracies, are ambivalent about the Net. On the one hand, they see it as a symbol of modernity and an engine for economic growth which may change the balance of economic advantage in their country's favour. On the other hand, they perceive it as a potentially destabilising force, undermining traditional political and legal structures, facilitating subversion, and eroding official control of what is published and read within their jurisdictions. They are also concerned at the potential erosion of their tax bases as a result of information goods crossing their frontiers as undetected (and untaxed) bitstreams.

Authoritarian responses. Governments differ greatly in the ways they react to what they see as the Internet's 'threats'. Authoritarian regimes generally attempt directly to control their populations' access to, and use of, the Net. A report by Reporters Sans Frontières (RSF) has identified 45 nations which impose blocking and filtering or all-out bans on Internet access (Reporters Sans Frontières 2000). Of the 45 nations, RSF said 20 could be described as real 'enemies of the Internet' for their actions. They are: the countries of central Asia and the Caucasus (Azerbaijan, Kazakhstan, Kirghizia, Tajikistan, Turkmenistan, and Uzbekistan), Belarus, Burma, China, Cuba, Iran, Iraq, Libya, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tunisia, and Vietnam. Many of the 20 nations are singled out for restrictions that make all Internet users access the network through a single, state-run ISP. These nations include Belarus, the nations of central Asia, Sudan, and Tunisia. The report singled out China for its close monitoring of Internet use despite the rapid pace with which Internet use is growing in that country. According to the *Economist* (2001: 25), China 'has

essentially covered its territory with an Intranet isolated from the rest of the world by software that blocks access to sites with unwanted content. Although clever surfers can tunnel through the "Great Firewall of China", it keeps the majority from straying too far online'. Most Chinese, in any case, access the Internet from work or public places where the state can control the software and track what they do online.

Other nations criticised for government-controlled filtering of the Internet included Iran, where, according to RSF, medical students are unable to access Web sites dealing with anatomy and where Internet access via any of Saudi Arabia's private ISPs goes through government filters that seek to maintain Islamic values.

The situation is even worse in other countries. The RSF report claimed that Internet access in Burma is available only through a state-run ISP and anyone who owns a computer must declare it to the government or face the possibility of a 15-year jail sentence if the machine is discovered. In Vietnam all Internet use has to be approved by the government through permits from the interior ministry and access is via state-run ISPs. And citizens of Iraq, Libya, North Korea, and Syria have no direct access to the Internet and even the official sites of the governments of these countries are maintained on servers overseas.

Pre-emptive legislation. More liberal administrations aim to reassert control by passing legislation which defines certain kinds of online activities as illegal, and then relying on the 'force of law' and the reluctance of ordinary citizens and ISP companies to become martyrs for liberty or freedom of speech to bring about the desired level of regulation. This is the approach favoured, for example, by the UK government, as demonstrated by its Regulation of Investigatory Powers Act 2000 (RIPA), which gives sweeping powers to the Home Secretary—that is, the minister of the interior—to intercept and read e-mail and other online traffic. RIPA gives the authorities the power to require an individual, on pain of imprisonment, to surrender the plaintext of an encrypted message or the key needed to decrypt it. A further provision makes it an offence punishable by five years in prison to reveal to a third party that she or he has been served with a decryption notice. The Act allows the Home Secretary to require ISPs to install a monitoring computer which is hardwired to a surveillance centre at MI5 headquarters, thereby enabling the authorities to gather *all* the bit traffic flowing through the servers of bugged ISPs and, when armed with the appropriate statutory order, to read the text of messages encoded in those monitored packets. It also gives the authorities the power to monitor an individual's 'clickstream', that is, the log of sites visited by that person on the Web, without having to seek a warrant.

RIPA has been described by the Director of the Foundation for Information Policy Research as 'the most draconian Internet surveillance law in the world' (Naylor 2001: 58). But although it is a piece of domestic UK legislation, it raises a number of wider issues which are of general relevance.

First, the fact that such an illiberal measure passed through the UK Parliament with relatively little difficulty and virtually no public debate stunned the UK Internet community. What it highlighted was the extent of legislators' ignorance of the issues involved in Internet regulation and the lack of public awareness of what was at stake. This is likely to be a pattern for the future in relation to Internet regulation, in that governments—and, on occasion, industry lobbies—will seek to make pre-emptive legislative strikes ahead of public opinion and before civil society activists can raise public awareness. Environmental campaigners have long experience of this official strategy.

Second, RIPA highlights the extent to which the Internet community underestimated the efficacy of new legislation in achieving anti-libertarian ends. All a sovereign government has to do is to pass legislation which defines specified activities as illegal. Unless the proposed restrictions are widely perceived as intolerable by the populace, they will be adhered to by the vast majority of people and by all companies involved in the area. The fact that some activists may become conscientious objectors or that others will find ingenious technological fixes which circumvent or defeat the proposed restrictions counts for little in the grand scheme of things. Governments would have found it difficult to impose their will on the original Internet community of researchers, programmers, and libertarians because they were less susceptible to pressure and technically adept at circumventing repressive measures; but the metamorphosis of the Net into a mass medium has transformed the possibilities for regulation and official intimidation.

Third, RIPA highlights the fact that the ISP has become a key choke-point in regulatory terms. All Internet users have to go through a service provider

in order to gain access to the Net. The vast majority of ISPs are private or public companies whose directors are obliged to obey the law and do their best to maximise shareholders' returns. This means that as corporate bodies they are disinclined to challenge legislation or legal action on principle. They see themselves as businesses and wish to be regarded, legally speaking, as common carriers rather than members of the Fourth Estate. Legislation such as RIPA which targets ISPs and requires them to cooperate with duly authorised surveillance measures is therefore likely to be very effective.

Fourth, RIPA is particularly revealing in the way it strikes at encryption: the technology that the Internet community has traditionally regarded as the ultimate guarantor of libertarian freedoms. Given that plain-text communications over the Net are intrinsically insecure, encryption is the only way of guaranteeing that private communications remain private. One could argue that, in the emerging online world, access to encryption tools becomes a basic human right and any infringement of that right must be circumscribed by law and a respect for the right to privacy enshrined in Article 8 of the European Convention on Human Rights and Fundamental Freedoms.

Historically, cryptography was something over which the state exerted total control. But the development of public key cryptography by university researchers in the 1980s created fresh waves of institutional paranoia about the subject (Levy 2000). The problem, as seen by governments, was that public key cryptography gave companies and private individuals access to strong encryption, with the result that law-enforcement, security, and surveillance services might therefore find themselves at a disadvantage with respect to the citizenry.

Most governments seem to have conceded that, technically speaking, the encryption genie has escaped from the bottle. In the Internet community this concession was interpreted as a historic victory. But such celebrations may be premature. RIPA suggests that instead of trying to crack codes surreptitiously governments will concentrate instead on putting legal pressure on individuals and companies. And the chances are that this approach will be highly effective: how many people will make a principled refusal to surrender a decryption key when the consequence of doing so is a two-year prison term?

The encryption issue is particularly important for civil society groups, some of which use the Net precisely as a way of short-circuiting or outflanking corporations and governments. Common sense suggests that they should encrypt their more sensitive communications. Yet doing so may leave them vulnerable to pressures under measures like RIPA. The old assumption—that strong encryption provided everyone with the only tool necessary to protect their privacy—has given way to the realisation that the tool has to be embedded in a politico-legal system which balances rights and responsibilities in some reasonable and accountable way.

The unexpectedly long arm of the law. The heady days when people believed that the Internet's transcendence of national boundaries would render it immune to conventional legal pressures is giving way to a more realistic appraisal of the power of legal codes to control online behaviour and to a more informed appraisal of the power of the nation state. As with encryption, the legal system seeks out critical points in the system and applies pressure on them. Once again, the ISP is a key target. In 2000, for example, a university teacher sued Demon Internet, a British ISP, because it had continued to relay Usenet news-groups in which allegedly defamatory comments about him were posted, despite previous complaints from him. Demon lost the case and then appealed, but withdrew from the appeal at the last minute, paid damages to the plaintiff—and established a legal precedent in the UK. This says that an ISP is legally bound to remove Usenet postings (or Web sites) if an individual alleges that material published therein is defamatory (Akdeniz 1999).

This has opened up an interesting can of worms; and the effects of this precedent are being felt already by campaigning civil society organisations. For example, a London pressure group campaigning for imaginative use of a disused power station castigated the new owners of the property for failing to proceed quickly with their plans for rejuvenating the building. A letter from the owners' solicitor to the ISP hosting the pressure group's Web site was sufficient to persuade the service provider to pull the site, 'just to be on the safe side'. Use of the law for purposes like this, which are essentially intimidatory, is certain to increase and is likely to cramp the freedoms of many campaigning organisations.

Other examples of the powers of national or international legislation to influence online behaviour include: the decision of a French court to require Yahoo!, an American company, to filter its auction

sites selling Nazi memorabilia so that French Web users could not access them; new EU laws which enable European consumers to sue EU-based Internet sites in their own countries; the endorsement by the US of the Council of Europe's Cybercrime treaty, which aims to harmonise laws against hacking, online fraud, and child pornography; and the way the US Digital Millennium Copyright Act has been used to intimidate, for example, authorities at Oxford University into deleting the Web pages of a student who was pretending to publish on his site the code of DeCSS, a computer program written to enable DVD disks to be played on computers running the Linux operating system.

What these developments suggest is that the early heady rhetoric about the futility of attempts to apply geographically-based legal regulation to non-geographical online activities was unduly optimistic and complacent. The truth is that, as Goldsmith has argued, libertarians have tended to 'overstate the differences between cyberspace transactions and other transnational transactions' and to 'underestimate the potential of traditional legal tools and technology to resolve the multi-jurisdictional regulatory problems implicated by Cyberspace' (Goldsmith 1999). Or, as the Economist (2001: 27) puts it, 'The Internet could indeed become the most liberating technology since the printing press—but only if governments let it'.

The Politics of Architecture: The 'Invisible Hand' of E-Commerce

As we noted earlier, many of the features of the Internet which make it particularly conducive to civil society applications are a product of the network's technological architecture. But if the underlying architecture were to change, then its usefulness to civil society might be reduced. There are compelling reasons to suppose that the rapid development of e-business poses a major threat because online commerce requires modification of the existing 'permissive' architecture in ways that will make it a more controlled space.

The problem is that a space in which 'nobody knows you're a dog' is not an environment in which one can safely trade. E-commerce requires security, authentication, and confirmation of transactions. An online trader needs to know with whom he or she is dealing; messages and transactions have to be secure from surveillance and interference; contracts have to be legally enforceable and incapable of arbitrary repudiation; ways have to be found for appending 'digital signatures' which have legal validity to electronic documents; and so on.

Technical solutions exist for all of these requirements, though many of them are currently rather clumsy. But the economic imperatives of online commerce are so urgent that significant improvements in the necessary protocols are under way. An entire new technical architecture to facilitate e-commerce is being created, in other words, ready to be grafted onto the older, libertarian architecture of the Net. And therein lies the danger.

The implication is that the Internet in 2005, say, could look very different from the Internet as it was in 1995. The old, libertarian layer will still exist, but a new layer—the e-commerce stratum—will sit above it. And the values implicit in the architecture of this new layer will be radically different from those embodied in the old one.

The key difference will be that the new layer will adapt the technical facilities of the old layer to eliminate anonymity and erode privacy. To understand how this will happen, you have to know something about how the Net operates. At present, every machine on the network has a unique address for the duration of its connection, and every transaction that machine conducts leaves a record. When an individual requests a Web page from a site, for example, the address of the requesting machine and the nature of its request are logged by the server. Anyone who runs a Web site can therefore find out the address of every machine which has accessed his or her site.[11] What they cannot ascertain, however, is the identity of the persons who initiated those accesses.

But the new e-commerce layer could change all that. It would enable sites, for example, to refuse access to people who refused—or were unable—to provide a digital signature authenticating their identity. Once admitted, everything those authenticated visitors did—which Web pages they viewed and for how long, which items they purchased, what they appeared to be most interested

[11] *As noted earlier, computers attached to a local area network may access the Net via a single 'gateway' machine whose IP address is the one that will show up in server logs. But the principle of machine traceability remains because in general it will be possible to identify an individual machine from an examination of server and gateway logs of the kind that might be demanded during a legal discovery process.*

in, and so on—can be logged against their real identities. And of course the information thus gathered could be sold or disclosed to other agencies—and all without the subjects' knowledge or consent. And because all the data gathered within such a layer would be in machine-readable form, it would be technologically and economically feasible to compile massive databases on the online behaviour of named individuals.

This possibility will be further reinforced by forthcoming changes to the Internet's address space. The explosive growth of the Net means that the world is rapidly running out of Internet addresses. Accordingly, a new version of the address protocol—IPv6—is now being implemented. This provides a vast address space but also includes a provision for an expanded IP number, part of which is the unique serial number of each computer's network-connection hardware, thereby making it possible in principle to track the online behaviour of every connected device.

The erosion of privacy implicit in such systems is an obvious danger. Less obvious, perhaps, is their potential for limiting access and widening the 'digital divide' between those who have a foothold in the new economy and those who do not. Apologists for the new e-commerce layer point out that nobody will be forced to have a digitally-authenticated signature and that they don't have to visit any site which requires one. True. Neither is there an obligation on anyone to have a credit card; but try renting a car or checking into an hotel nowadays without one.

Add to the authentication threat the provisions for digital copyright which the publishing industries are demanding from legislatures around the world, and one can see the makings of an Orwellian nightmare. When the Web first took off and it became easy to copy any text and distribute it globally, publishers—and in some cases authors—feared that it spelled ruination for them. It was, they argued, a charter for intellectual piracy, the equivalent of putting a photocopier and a printing press into every home. It hasn't turned out like that, but one can see why they were alarmed because, with an anonymous Net, everything they feared was technically possible.

But spool forward a few years and change the architecture and an entirely new scenario presents itself. Suddenly the balance of power has shifted. Every document published on the Web can be encrypted, so that only readers who have paid for a decryption key can access it. Alternatively, an unencrypted document can have a secret 'digital watermark' embedded in it, enabling publishers to tell at once whether a given digital copy is a legitimate, paid-for version or a pirated one. And even if the document is published free, unencrypted, and unmarked, on a Net where authentication protocols are in place the publisher could determine the precise identity of every single person who accesses the document online—and sell that information to other customers or abuse it in other ways. With such an architecture, the practice of anonymous reading—one of the great bulwarks of intellectual freedom—could be rendered impossible, at least in relation to online documents.

The inescapable implication is that cyberspace—the most open, uncensored and unregulated public space in human history—could easily become the most controlled environment imaginable. Or, to use Lessig's (1999*b*: 6) phrase, 'the invisible hand of cyberspace is building an architecture that is quite the opposite of what it was at cyberspace's birth. The invisible hand, through commerce, is constructing an architecture that perfects control'.

New Technologies—and New Possibilities?

The history of disruptive technologies—think of the automobile—is often one of ongoing dialectical struggle between technical innovation and social control. New developments create new possibilities, and with them new threats to the established order; there follows a period of chaos, innovation, and change while the old order is thrown into apparent disarray; then, after a burst of institutional reform and adaptation, a measure of social control is reasserted over the disruptive technology. And so the process goes on.

Looking at the Internet from this perspective, we can see a similar pattern. We are currently living through a period in which the established order, after a relatively brief period of denial and confusion, appears to be asserting control over the technology. But at the same time new technologies are emerging which may once again prove disruptive. Many of these technologies fall under the general banner of 'peer-to-peer' networking. To understand their potential significance, it's helpful to portray the development of the network in three phases. Let us call them Internet 1.0, 2.0, and 3.0.

Internet 1.0

From its inception in 1983 to about 1994, the entire Internet had a single model of connectivity. There were relatively few dial-up connections. Machines were assumed to be always on, always connected, and assigned permanent IP addresses. The Domain Name System (DNS)—the system which relates domain names like www.cnn.com to a specific Internet address (in this case 207.25.71.30)—was designed for this environment, where a change in IP address was assumed to be abnormal and rare, and could take days to propagate through the system. Because machines had persistent connections and fixed addresses, every machine on the network could function as a server. It was a genuine network of *peers*, that is, machines of equal status.

Internet 2.0

The World Wide Web was invented at CERN by Tim Berners-Lee in 1990, but the first popular Web browser was *Mosaic*, created at the National Center for Supercomputing Applications at the University of Illinois in 1993. With the appearance of *Mosaic* and the subsequent appearance of the Netscape browser in 1994, Web use began to grow very rapidly (Naughton 2000: 248) and a different connectivity model began to appear. To run a Web browser, a PC needed to be connected to the Internet over a modem, with its own IP address. This created a second class of connectivity because PCs did not have persistent connections and would enter and leave the network frequently and unpredictably.

Furthermore, because there were not enough unique IP addresses available to handle the sudden demand generated by *Mosaic* and Netscape, ISPs began to assign IP addresses dynamically, giving each PC a new, temporary IP address for the duration of each dial-up session. A subscriber might therefore be assigned a different IP address every time she logged on to the Net. This instability prevented PCs from having DNS entries and therefore precluded their users from hosting any data or Net-facing applications locally, that is, from functioning as servers. They were essentially clients: machines which requested services (files, Web pages, and so on) from servers.

For a few years, the connectivity model based on treating PCs as dumb clients worked tolerably well. Indeed, it was probably the only model that was feasible at the time. Personal computers had not been designed to be part of the fabric of the Internet, and in the early days of the Web the hardware and unstable operating systems of the average PC made it unsuitable for server functions.

Internet 2.0 is still the model underpinning the Internet as we use it today. It is essentially a two-tier networked world made up of a minority of 'privileged' machines—servers within the DNS system with persistent, high-speed connections and fixed IP addresses—providing services to a vast number of dial-up machines which are essentially second-class citizens because they cannot function as servers and have an IP address only for the duration of their connection to the Net. Such a world is, as we have seen, potentially vulnerable to governmental and corporate control for, if everything has to happen via a privileged server and servers are easy to identify, then they can be targeted for legal and other kinds of regulation.

Internet 3.0: a distributed Peer-to-Peer network?

Internet 2.0 made sense in the early days of the Web. But since then the supposedly 'dumb' PCs connected to the Net have become immeasurably more powerful and the speed and quality of Internet connections have steadily improved, at least in the industrialised world. On the software side, not only have proprietary operating systems improved but the Open Source—that is, free—software movement has produced increasingly powerful operating systems (for example, Linux) and industrial-strength server software (for example, the Apache Web server program which powers over half the world's Web sites even on commercial servers). As a result, it has become increasingly absurd to think of PCs equipped in this way as second-class citizens.

It is also very wasteful to use such powerful machines simply as life-support systems for a Web browser. The computing community realised quite quickly that the unused resources existing behind the veil of second-class connectivity might be worth harnessing. According to Shirky (2001: 23), the world's Net-connected PCs presently possess an aggregate 10 billion MHz of processing power and 10,000 terabytes (trillions of bytes) of storage. And this is a conservative estimate because it assumes only 100 million PCs among the net's 300 plus million users, and only a 100 MHz processor and 100 Mb drive on the average PC.

Box 6.1: Napster

Napster provided downloadable software that made it easy for Internet users to trade MP3 files with one another. Subscribers downloaded a small client program which communicated with Napster servers whenever a machine connected to the Net and updated a database with details of MP3 tracks on the machine's hard disk which the owner had designated as being available for sharing. The Napster service worked by constantly updating a master song list, adding and removing songs as individual users connected and disconnected their PCs. When someone requested a particular song, the Napster server initiated a direct file transfer from a user who had a copy of the song to the user who requested it. The service proved wildly popular with users; it built up a subscriber base of nearly 60 million users in its first 18 months of existence. Since much of the music content in the Napster system was copyrighted, the multinational record companies took legal action to close down the service in its original form. This action was predictably successful: because the system depended on having a central database, it was always likely to be vulnerable to legal attack.

Early attempts to harness these distributed resources were projects like SETI@Home (URL) in which PCs around the globe analysed astronomical data as a background task when they were connected to the Net. More radical attempts to harness the power of the network's second-class citizens have been grouped under the general heading of 'peer-to-peer' (P2P) networking. This is an unsatisfactory term because, strictly speaking, the servers within the DNS system have always interacted on a peer-to-peer basis, but it has been taken up by the mass media and is likely to stick.

The best available definition of P2P is Shirky's description of it as 'resource-centric addressing for unstable environments'. In this view:

> *P2P is a class of applications that takes advantage of resources—storage, processing cycles, content, human presence—available at the edges of the Internet. Because accessing these decentralized resources means operating in an environment of unstable connectivity and unpredictable IP addresses, P2P nodes must operate outside the DNS system and have significant or total autonomy from central servers.* (Shirky 2001: 22)

The most widely-known P2P application to date is Napster (see Box 6.1). Although Napster may fade away following its failure to win the legal battle over the propriety of its service, it has served as a seminal influence in several ways. First, it triggered a realisation that PCs on the periphery of the Net might be capable of more ambitious things than merely requesting Web pages from servers. Second, it overturned the publishing model of Internet 2.0: the idea that content had always to be obtained from the magic circle within the DNS system. Instead Napster pointed to a radically different model, which Shirky (2000) calls 'content at the edges'. The current content-at-the-centre model, he writes, 'has one significant flaw: most Internet content is created on the PCs at the edges, but for it to become universally accessible, it must be pushed to the center, to always-on, always-up Web servers. As anyone who has ever spent time trying to upload material to a Web site knows, the Web has made downloading trivially easy, but uploading is still needlessly hard'.

Napster relied on several networking innovations to get around these limitations. First, it dispensed with uploading and left the files on the PCs, merely brokering requests from one PC to another: the MP3 files did not have to travel through any central Napster server; second, PCs running Napster did not need a fixed Internet address or a permanent connection to use the service; and third, it ignored the reigning paradigm of client and server. Napster made no distinction between the two functions: if you could receive files from other people, they could receive files from you as well.

Finally, Napster pointed the way to a networking architecture which re-invents the PC as a hybrid client-

plus-server while relegating the DNS-governed centre of the Internet, where all the action had hitherto taken place, to nothing but brokering connections.

Because of its reliance on a central server, Napster proved vulnerable to legal measures. But other, genuinely distributed P2P technologies now exist which may be less susceptible to challenge. Gnutella (URL), Freenet (URL), and Publius (URL), for example, are three file-distribution systems which use the resources of machines at the edge of the Internet to store and exchange files without relying on any centralised resource.[12]

From a civil society perspective, Publius (Waldman, Cranor, and Rubin 2001) is particularly interesting. It is a Web publishing system designed to be very resistant to censorship and to provide publishers with a high degree of anonymity. It was originally developed by programmers working for AT&T and named after the pen name used by the authors of the Federalist Papers: Alexander Hamilton, John Jay, and James Madison. This collection of 85 articles, published pseudo-nymously in New York State newspapers in 1787–88, was influential in persuading New York voters to ratify the proposed United States constitution.

Publius encrypts and fragments documents, then randomly places the pieces, or keys, on to the servers of volunteers in a variety of locations worldwide. The volunteers have no way of knowing what information is being stored on their servers. Software users configure their browser to use a proxy, which will bring the pieces of the document back together. Only a few keys out of many possibilities are needed to reconstruct a document. The inventors of the system claim that even if 70 per cent of the Publius sites are shut down, the content is still accessible. Only the publisher is able to remove or alter the information (Waldman, Cranor, and Rubin 2001: 153).

It is impossible to know at this stage whether P2P technologies will indeed 'turn the Internet inside out', as (Shirky 2000) has put it. But they already offer potentially powerful tools to groups which are interested in the free exchange of ideas and files online, especially if those ideas or files are likely to be controversial. Rubin, for example, has declared that his greatest hope is that Publius will become an instrument for free speech, a tool that could enable dissidents living under oppressive governments to speak out without fear of detection or punishment (quoted in Shreve 2000). Having said that, we must remember that, as ever, technology is a necessary but not sufficient condition for liberation. The benefits of P2P will not be evenly distributed. It will work for groups in countries that are neither too poor nor too completely totalitarian to allow some access. Thus, P2P has potential for Singapore and Malaysia but much less for, say, Zimbabwe or North Korea. Libertarianism may have discovered a new tool kit. But economic, social, political, and cultural factors will determine who gets to use it.

Conclusion

This chapter has argued that the Internet offers valuable facilities to global civil society and has shown that these facilities have been imaginatively used by many groups outside the corporate and governmental worlds to foster understanding and action on human rights, sustainable development, the environment, and other important issues. We have also seen that the democratising potential of the Net is undermined by the digital divide and that the chasm between the 'information rich' in the industrialised countries and the 'information poor' in the rest of the world is alarmingly wide. What this means is that measures to understand and redress the imbalance ought to be an integral part of debates on economic, social, and cultural development.

Thus far, global civil society has been almost entirely instrumental in its attitudes to the Internet. It has assumed that the network is a 'given' and that the only challenge is to make effective use of it. This view is profoundly misguided. The Internet is the way it is—open, permissive, uncontrolled by governments and corporations—because of the values embodied in its technical architecture. These values resonate with those of global civil society. But there are powerful forces, representing very different values, which are pressing to change the architecture to make the system much more closed and controllable. Such changes would be disastrous for those who seek to use the Net for informing, communicating, and campaigning against governmental and corporate power. The danger is that civil society groups might one day discover that the network has evolved into something less congenial to their needs and purposes.

In some ways, what we are discovering is not how different cyberspace is from the real world but how

[12] *Oram (2001) contains useful articles by developers of all three systems.*

alike the two spaces are. Many of the tensions between civil society and corporate and governmental power that characterise the real world are beginning to manifest themselves in the virtual one. And this is true not just in relation to security, surveillance, control, and intellectual property but also in terms of software and infrastructure. It is vital, for example, to ensure that the Internet continues to be based on open, non-proprietary protocols and that companies like Microsoft are not allowed to leverage their market power to dominate the system. And it is important to realise that the values which drive the Open Source movement resonate powerfully with the values which motivate civil society groups (Di Bona, Ockman, and Stone 1999; Bollier 1999).

Mitch Kapor, one of the founders of the Electronic Frontier Foundation, articulated an important truth in his famous observation that 'architecture is politics' (Kapor 1990). So it is. And so too is software because that is the material from which the Internet is constructed. Global civil society has a vital stake in ensuring that the values which shaped the original Internet remain at the heart of its evolving architecture. The struggle to keep it open, free, permissive, and uncontrolled is too important to be left just to geeks and engineers.

References

Akdeniz, Y. (1999). 'Case Analysis: Laurence Godfrey v. Demon Internet Limited'. *Journal of Civil Liberties*, 4: 260–7.

Arnett, Elsa C. (1999). 'Seattle Protests Put a New Activism in Play'. *San Jose Mercury News*, 3 December. Available at http://www./globalexchange.org/wto/sjmerc120399.html

Barlow, John Perry (1996). A Declaration of the Independence of Cyberspace. http://www.eff.org/~barlow/Declaration-Final.html

—, Birkerts, Sven, Kelly, Kevin, and Slouka, Mark (1995). 'What are we doing online?'. *Harper's*, August.

Bollier, David (1999). 'The Power of Openness: A Critique and a Proposal for the H2O Project'. Available at http://www.opencode.org/h2o/, 10 March.

BSE. http://www.bse.org.uk

Case, Alyssa (1999). 'The Role of the Internet in Human Rights Development' (M. Phil. dissertation). Cambridge: Centre for International Studies, University of Cambridge.

Derechos Human Rights. http://www.derechos.org/human-rights/manual.htm

Di Bona, Chris, Ockman, Sam, and Stone, Mark (eds) (1999). *Open Sources: Voices from the Open Source Revolution*. Sebastapol: O'Reilly and Associates.

Economist (2001). 'The Internet and the Law: Stop Signs on the Web'. 13 January.

FAST. http://www.amnestyusa.org/stoptorture/fast/fastindex.html

Freenet. http://www.freenet.sourceforge.net

Gilmore, John (1996). *New York Times*, 15 January.

GreenNet, 'The Civil Society Internet Charter'. http://www.gn.apc.org/action/csir/charter.html.

Goldsmith, Jack L. (1999). 'Against Cyberanarchy'. University of Chicago Law School, Occasional Paper No. 40, August 13. Available at http://www.law.uchicago.edu/Publications/Occasional/40.html

Gnutella. http://www.gnutella.wego.com

Google. http://www.google.com

Hafner, Katie and Lyon, Matthew (1996). *Where Wizards Stay Up Late: The Origins of the Internet*, New York: Simon and Schuster.

International Telecommunications Union (1998). http://www.itu.int/sg3focus/teledensityA.htm

Introna, Lucas and Nissenbaum, Helen (2000). 'The Public Good Vision of the Internet and the Politics of Search Engines', in Richard Rogers (ed.), *Preferred Placement: Knowledge Politics on the Web*. Maastricht: Jan Van Eyck Editions.

IRC. http://www.mirc.com/irc.html

Kapor, Mitch (1990), 'The Software Design Manifesto', Available online at http://www.kei.com/homepages/mkapor/Software_Design_Manifesto.html

Kestemont, B. (1998). 'Best Environmental Directories', available at http://www.ulb.ac.be/ceese/meta/cds.html

Kobrin, Stephen (1998). 'The MAI and the Clash of Globalizations'. *Foreign Policy*, 112/Fall.

Kollock, Peter and Smith, Marc A. (1999). 'Communities in Cyberspace', in Marc A. Smith and Peter Kollock (eds), *Communities in Cyberspace*. London: Routledge.

Lessig, Lawrence (1999*a*). 'Open Code and Open Societies: The Values of Internet Governance' (1999 Sibley Lecture, 16 February). Athens: University of Georgia.

— (1999*b*). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Levy, Stephen (2000). *Crypto: Secrecy and Privacy in the New Code War*. London: Allen Lane.
Miller, Daniel and Slater, Don (2000). *The Internet: An Ethnographic Approach*. Oxford: Oxford University Press.
Mitchell, William (1995). 'Public Life in Electropolis: Dialog on Virtual Communities'. http:// www.feedmag.com/95.08dialog/95.08dialog1.html
Naughton, John (2000). *A Brief History of the Future: The Origins of the Internet*. London: Phoenix.
Naylor, Lisa (2001). 'The Wrong Arm of the Law'. *The Industry Standard Europe*, 8/ March: 58–9.
Nua Internet Surveys. http://www.nua.ie
OneWorld. http://www.oneworld.net/about/partnership_principles.shtml
Oram, Andy (ed.) (2001). *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Sebastapol: O'Reilly and Associates.
Peizer, Jonathan (2000). 'Bridging The Digital Divide: First You Need The Bridge'. http://www.mediachannel.org/views/oped/peizer.shtml, 21 June.
The Pew Internet and American Life Project. http://www.pewinternet.org/reports/chart.asp?img=6_daily_activities.jpg
Publius. http://www.publius.cdt.org
Reporters Sans Frontières (2000). 'The Enemies of the Internet'. http://www.rsf.fr/uk/html/internet/ennemis.html
Rheingold, Howard (1995). 'Public Life in Electropolis: Dialog on Virtual Communities'. http://www.feedmag.com/95.08dialog/95.08dialog1.html
SETI@Home. http://www.setiathome.ssl.berkeley.edu
Shayler, David. http://www.guardianunlimited.co.uk/shayler/
Shirky, Clay (2000) 'Content Shifts to the Edges'. http://www.shirky.com/writings/content.html, April.
— (2001). 'Listening to Napster', in Andy Oram (ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Sebastapol: O'Reilly and Associates.
Shreve, Jenn (2000). 'Avi Rubin: Publius' Public Crusade'. *The Industry Standard*, 13 September. Available at http://www.thestandard.com/article/0,1902,18487,00.html
Stanford Center for Internet and Society (2000). 'The Policy Implications of End-to-End', 1 December. Proceedings available online at http://lawschool.stanford.edu/e2e/
UNDP (1999). *Human Development Report 1999*. New York: United Nations.
Waldman, Marc, Cranor, Lorrie Faith, and Rubin, Avi (2001). 'Publius', in Andy Oram (ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Sebastapol: O'Reilly and Associates.
Wellman, Barry and Milena, Gulia (1999). 'Virtual Communities as Communities', in Marc A. Smith and Peter Kollock (eds), *Communities in Cyberspace*. London: Routledge.